UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JULIE COLBY, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

SHIELDS HEALTH CARE GROUP INC.,

Defendant.

Civil Action No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Julie Colby ("Plaintiff"), on behalf of herself and all others similarly situated, alleges, by and through her undersigned counsel, the following against Shields Health Care Group Inc. ("Shields" or "Defendant"), based upon her personal knowledge with respect to herself and her own acts, and upon information and belief, upon her own investigation and the investigation of her counsel, as to all other matters, as follows:

I. INTRODUCTION

1. Shields is a provider of healthcare services in the New England region, including Massachusetts, Maine, Rhode Island, and New Hampshire. Shields provides MRI, PET/CT, and ambulatory surgical services to patients at more than 40 locations in New England.

2. On or about June 7, 2022, Shields announced a security incident involving the personally identifiable information ("PII") and protected health information ("PHI") of its patients (collectively, "Private Information").[1] The exposed Private Information may have included

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created,

patients' names, dates of birth, home address, provider information, diagnosis, Social Security numbers, billing information, insurance number and information, medical record number, patient ID and other medical or treatment information (the "Data Breach"). Although the Data Breach occurred between March 7, 2022, to March 21, 2022. Shields waited three months before notifying patients in June 2022.

3. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Private Information. In particular, the Private Information was maintained on Shields' computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Shields, and thus Shields was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position. In fact, Shields had been the subject of a data breach attack through Accellion only a few months earlier.

4. Defendant disregarded the rights of Plaintiff and Class Members by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to

---

collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule, available at*: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed July 20, 2022).

disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard patients' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice regarding the Data Breach.

5. As a result of Defendant's failure to implement and follow reasonable security procedures, Plaintiff's and Class Members' Private Information is now in the hands of, and has been viewed by, identity thieves. Plaintiff and Class Members have suffered or will suffer identity theft, fraud and other damage as a consequence of the Data Breach, have had to spend and will continue to spend significant amounts of time and/or money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party.

7. Plaintiff, on behalf of all others similarly situated, alleges claims for common law and statutory violations.

8. Plaintiff seeks remedies including, but not limited to, compensatory damages for identity theft, fraud, and time spent, reimbursement of out-of-pocket costs, adequate credit monitoring services funded by Defendant, and injunctive relief including improvements to Defendant's data security systems and practices to ensure they have reasonably sufficient security

practices to safeguard patients' Private Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

II. PARTIES

9. Plaintiff Julie Colby is a resident of Lewiston, Maine, and a Shields patient. In June of 2022, Plaintiff received notice from Shields that her Private Information had been improperly exposed to unauthorized third parties.

10. Defendant Shields is a Massachusetts corporation with its principal place of business in Quincy, Massachusetts. Shields is a provider of health care that has more than 40 facilities throughout New England, offering MRI, PET/CT, and outpatient surgical services.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

13. This Court has personal jurisdiction over Defendant because Shields is headquartered in Massachusetts, its principal place of business is in Massachusetts, and it regularly conduct business in Massachusetts.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a Defendant resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, Shields is based in this District, Shields maintain patients' Private Information in the District, and have caused harm to Plaintiff and Class Members residing in this District.

IV. STATEMENT OF FACTS

A. Shields' Business.

15. In 1972, Tom and Mary Shields owned and operated the Madalawn Nursing Home in Brockton, Massachusetts. Over the next 10 years, Tom and Mary established the largest regional dialysis center in New England and opened the first independent regional MRI center in 1986. Presently, Shields has more than 40 facilities throughout New England, offering MRI, PET/CT, and outpatient surgical services.

16. Due to the nature of its services, Shields must store patients' Private Information in its system. Shields accomplishes this by keeping the Private Information electronically, as evidenced by this Data Breach.

17. Patients demand security to safeguard their Private Information. As a healthcare provider, Shields is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express, written consent, as further detailed below.

B. The Data Breach.

18. Beginning on or around March 7, 2022 to March 21, 2022, unauthorized parties accessed the computer system of Shields and acquired Plaintiff's and Class Members' Private Information. For a couple of weeks, unauthorized parties maintained uninterrupted access to the Private Information of Shields' patients, including Plaintiff and Class Members.

19. After learning of the issue, Shields commenced an investigation. That investigation revealed that approximately two million patients were victims of the cybersecurity attack. The investigation further revealed that information accessed by the hackers includes patients' names, medical information, information related to their use of Shields' services, Social Security numbers,

and other Private Information that Shields collected and maintained.

20. Defendant did not inform patients of this Data Breach until June 7, 2022, in a press release stating that the following information had been breached:

> "Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information." ("Notice").[2]

21. The Notice disclosed that there had been unauthorized suspicious activity on its network between March 7, 2022, to March 21, 2022. Shields did not discover this until March 28, 2022. The Notice indicated that the "suspicious activity may have involved data compromise" and that Shields "immediately launched an investigation into this issue…"[3]

22. The Notice further informed patients that:

> This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time
>
> Shields takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we took steps to secure our systems, including rebuilding certain systems, and conducted a thorough investigation to confirm the nature and scope of the activity and to determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we continue to review and further enhance these protections as part of our ongoing commitment to data security. [4]

[2] Shields Health Care Group, Notice of Data Security Incident, available at https://shields.com/notice-of-data-security-incident/ (last accessed July 20, 2022).

[3] *Id.*

[4] *Id.*

23. It took Shields nearly three months after the Data Breach to inform Plaintiff and Class Members of the Data Breach, resulting in Plaintiff and Class Members suffering harm they otherwise may have been able to avoid had Shields announced the Data Breach sooner.

24. Shields' Notice of Data Breach was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed its computer server, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many patients were affected by the Data Breach. Even worse, Shields failed to offer even a single year of identity monitoring to Plaintiff and other Class Members.

25. Plaintiff's and Class Members' Private Information is likely for sale to criminals on the dark web meaning unauthorized parties have accessed and viewed Plaintiff's and Class Members' unencrypted, unredacted information, including name, date of birth, billing and insurance information, patient referral information, relevant medical records, diagnosis information, Social Security numbers, and more.

C. Plaintiff's Efforts to Secure Their Private Information.

26. Plaintiff has been regularly using Shields imaging, located in Topsham, Maine for her annual mammograms for a number of years. On December 15, 2021, Plaintiff went to Shields for a chest x-ray.

27. Plaintiffs PII and PHI was available to Shields through either her doctor's office, and/or Central Maine Healthcare, with which her doctor is associated, and which provided her PII and PHI to Shields.

28. Plaintiff received a letter informing her of the Data Breach sometime in June, 2022.

29. Thereafter, Plaintiff spent time taking action to mitigate the impact of the Data Breach after she received the Shields Notice, which included diligently checking her accounts and her financial accounts. This is time Plaintiff otherwise would have spent performing other activities or leisurely events for the enjoyment of life.

30. Subsequent to the Data Breach, Plaintiff was subject to a potential fraud concerning her health insurance. Specifically, after the Data Breach, Plaintiff received two calls, one during the evening of June 28, 2022, and another during the evening of July 8, 2022, in which the caller was attempting to reach her to purportedly speak to her about her health insurance plan. Both calls were from the same phone number. Upon receiving these calls, Plaintiff researched the telephone number on the internet and determined that the calls were made from a scammer who likely had access to information about her health insurance plan.

31. Since the Data Breach, Plaintiff has further received an increase in spam telephone calls. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her protected health information which she expected Shields to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his personal and medical information.

32. Plaintiff suffered actual injury from having her Private Information exposed as a result of the Data Breach including, but not limited to (a) paying monies to Shields for its goods and services which she would not have paid had Shields disclosed that it lacked data security practices adequate to safeguard patients' Private Information from theft; (b) damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Shields as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

33. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

D. Shields' Privacy Policies.

34. In Shields' Privacy Practice statement on its website at shields.com/privacy/ it states that it is their responsibility as a provider to "Maintain the privacy of your health information as required by law." In addition, Shields states in its Notice of Data Security Incident on its website at shields.com/notice-of-data-security-incident/ that "Shields takes the confidentiality, privacy, and security of information in our care seriously."

35. Shields also describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

36. By failing to protect Plaintiff's and Class Members' Private Information, and by allowing the Data Breach to occur, Shields broke these promises to Plaintiff and Class Members.

E. The Healthcare Sector is Particularly Susceptible to Cyberattacks.

37. Defendant was on notice that companies in the healthcare industry were targets for cyberattacks especially since it was involved in the Accellion data breach.

38. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or

Personally Identifiable Information (PII)."[5]

39. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[6]

40. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[7] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[8] That trend continues.

41. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[9] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity

---

[5] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited July 20, 2022).

[6] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited July 20, 2022).

[7] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed July 20, 2022).

[8] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed July 20, 2022).

[9] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed July 20, 2022).

theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[11]

42. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[12] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[13]

43. As a healthcare provider, Shields knew, or should have known, the importance of safeguarding the patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This is especially true given its involvement in the

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 20, 2022).

[11] *Id.*

[12] *2019 HIMSS Cybersecurity Survey*, *available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed July 20, 2022).

[13] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed July 20, 2022).

Accellion data breach. This includes the significant costs that would be imposed on Shields' patients as a result of a breach. Shields failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Shields Acquires, Collects and Stores Its Patients' Private Information.

44. Shields acquires, collects, and stores a massive amount of its patients' protected health information and other personally identifiable data.

45. As a condition of engaging in health services, Shields requires that these patients entrust them with highly confidential Private Information.

46. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Shields assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

47. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former patients, they relied on Shields to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

G. The Value of Private Information and the Effects of Unauthorized Disclosure.

48. At all relevant times, Defendant were well aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

49. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including

identify theft, and medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

50. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[15]

51. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

52. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

---

[14] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed July 20, 2022).

[15] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed July 20, 2022).

[16] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited July 20, 2022).

53. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

54. The ramifications of Shields' failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

55. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

56. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[17] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[18]

57. As a healthcare provider, Shields knew, or should have known, the importance of

---

[17] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed July 20, 2022).

[18] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accesses July 20, 2022).

safeguarding its patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Shields' patients as a result of a breach. Shields failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

H. Shields' Conduct Violates HIPAA.

58. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[19]

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

60. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[20]

61. Based on information and belief, Defendant's Data Breach resulted from a

[19] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed July 20, 2022).

[20] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited July 20, 2022).

combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Shields' security failures include, but are not limited to, the following:

i. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

ii. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

iii. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

iv. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

v. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

vi. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

vii. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

viii. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

ix. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

x. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

I. Shields Failed to Comply with FTC Guidelines.

62. Shields was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[22] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

[21] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed July 20, 2022).

[22] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 20, 2022).

security problems.

65. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. Shields failed to properly implement basic data security practices. Shields' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

68. Shields was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. Shields was also aware of the significant repercussions that would result from its failure to do so.

J. Shields Failed to Comply with Healthcare Industry Standards.

69. HHS's Office for Civil Rights notes:

[23] FTC, *Start With Security*, *supra* note 16.

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[24]

70. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

71. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[25] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

72. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Shields chose to ignore them. These best practices were known, or should have been known by Shields, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

K. Plaintiff and Class Members Suffered Damages.

73. The ramifications of Shields' failure to keep patients' Private Information secure

---

[24] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed July 20, 2022).

[25] *See e.g.*, INFOSEC, *10 Best Practices For Healthcare Security*, *available at:* https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last accessed July 20, 2022).

are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[26]

74. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

75. Defendant further owed and breached its duty to Plaintiff and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

76. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff are now at a heightened and increased risk of identity theft and fraud.

77. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity

[26] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed July 20, 2022).

theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

78. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

79. The Plaintiff has not had her PII and PHI compromised through any other data breaches, to her knowledge.

80. Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in their agreements with Shields and they were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

81. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

82. The Private Information belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

83. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative,

technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

84. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

85. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

86. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

87. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[27]

88. In the Data Breach Notice, Shields has not offered or provided victims any identity monitoring services, fraud insurance or medical identity theft protection. Shields' fails to address the fact that victims of data breaches and other unauthorized disclosures commonly face multiple

[27] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 20, 2022).

years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

89. Defendant does not appear to be taking any measures to assist Plaintiff and Class Members other than telling them to simply take certain steps to protect their information and do the following:

- "Monitor Your Accounts";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff's and Class Members' Private Information.

90. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sit by and do nothing to assist those affected by the incident. Instead, as Shields' Data Breach Notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

91. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

i. The compromise, publication, theft and/or unauthorized use of their Private Information;

ii. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

iii. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

iv. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

v. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

vi. Anxiety and distress resulting from fear of misuse of their medical information.

92. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

L. Shields' Delay in Identifying & Reporting the Breach Caused Additional Harm.

93. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[28]

[28] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire¸ *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed July 20, 2022).

94. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[29]

95. Although their Private Information was improperly exposed on or about March 7-21, 2022, Plaintiff and Class Members were not notified of the Data Breach until June 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

96. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

V. CLASS ALLEGATIONS

97. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

98. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class: All individuals whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**

99. In the alternative to the Nationwide Class, Plaintiff seek certification of the

[29] Consumer Reports, *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed July 20, 2022).

following state Sub-Class:

> **Maine Sub-Class: All persons residing in Maine whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**

100. The Nationwide Class and Maine Sub-class are together referred to as the "Classes". Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

101. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Sub-class before the Court determines whether certification is appropriate.

102. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class, and State Subclass are so numerous that joinder of all members is impracticable. Defendant has identified over 1.2 million patients whose Private Information may have been improperly accessed in the Data Breach and at least hundreds of Maine residents whose Private Information was compromised, and the Class and Sub- class are apparently identifiable within Defendant's records.

103. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class and Sub-class exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

ii. Whether Defendant owed a duty to the Class and Sub-class to exercise due

care in collecting, storing, safeguarding and/or obtaining their Private Information;

iii. Whether Defendant breached that duty;

iv. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

v. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII/PHI;

vi. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

vii. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

viii. Whether Defendant caused Plaintiff's and Class Members' damages;

ix. Whether Defendant violated the law by failing to promptly notify Class and Sub-class Members that their Private Information had been compromised;

x. Whether Plaintiff and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

xi. Whether Defendant violated common law and statutory claims alleged herein.

104. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members and Sub-class members, because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

105. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class and Sub-class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and Sub-class Members and making final injunctive relief appropriate with respect to the Class and Sub-class as a whole. Defendant's

policies challenged herein apply to and affect Class and Sub-class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class and Sub-class as a whole, not on facts or law applicable only to Plaintiff.

106. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class and Sub-class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class and Sub-class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and Sub-class and the infringement of the rights and the damages they have suffered are typical of other Class and Sub-class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

107. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

108. The nature of this action and the nature of laws available to Plaintiff and the Class and Sub-class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class and Sub-class for the wrongs alleged because

Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class and Sub-class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

109. Shields is based in Quincy, Massachusetts, and on information and belief, all managerial decisions emanate from there, the representations on Shields' website originate from there, Shields' misrepresentations originated from Massachusetts, and therefore application of Massachusetts law to the Nationwide Class is appropriate.

110. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class and Sub-class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

111. Adequate notice can be given to Class and Sub-class Members directly using information maintained in Defendant's records.

112. Unless a Class-wide injunction is issued, Plaintiff and Class and Sub-class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiff and Class and Sub-class Members resulting in another data breach, continue to refuse to provide proper notification to Class and Sub-class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Complaint.

113. Defendant has acted or refused to act on grounds generally applicable to the Class

and Sub-class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class and Sub-class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

114. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

i. Whether Defendant owed a legal duty to Plaintiff and Class and Sub-class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

ii. Whether Defendant breached a legal duty to Plaintiff and Class and Sub-class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

iii. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

iv. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

v. Whether Class and Sub-class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

115. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

116. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Shields directly, or through their other healthcare providers, with their Private Information.

117. Plaintiff and Class Members entrusted their Private Information to Shields with the understanding that Shields would safeguard their information.

118. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

119. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure that Private Information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on relevant cybersecurity measures.

120. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Private Information, the current cyber scams being perpetrated, and that they had inadequate employee training and education and IT

security protocols in place to secure the Private Information of Plaintiff and Class Members.

121. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the Private Information of Plaintiff and Class Members.

122. Plaintiff and Class Members had no ability to protect their Private Information that was in Defendant's possession.

123. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

124. Defendant had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Members' Private Information.

125. Defendant has admitted that Plaintiff's and Class Members' Private Information was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

126. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information while it was within Defendant's possession or control.

127. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' Private Information in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

128. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and

prevent dissemination of its Plaintiff's and Class Members' Private Information.

129. Defendant, through their actions and/or omissions, unlawfully breached their duty to adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

130. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' Private Information would not have been compromised and/or subsequently misused by unauthorized third parties to engage in fraudulent activity further harming Plaintiff and Class Members.

131. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered, by Plaintiff and the Class.

132. As a result of Defendant's negligence, unauthorized parties acquired Plaintiff's Private Information and used that specific information to harm Plaintiff and Class Members as described above. As a further result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer damages and injury including, but not limited to, (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) diminished value of the Private Information; (f) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (g) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate

and adequate measures to protect Private Information in their continued possession; and (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

133. Violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se*.

134. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Shields, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

135. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

136. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

137. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

139. Defendant's violation of HIPAA also independently constitutes negligence *per se*. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

140. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

142. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

143. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT II
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

144. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

145. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

146. Defendant owed a duty to patients in their network, including Plaintiff and Class Members, to keep their Private Information confidential.

147. The unauthorized release of Private Information, especially the type related to personal health information, is highly offensive to a reasonable person.

148. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

149. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

150. Defendant acted with a knowing state of mind when they permitted the Data Breach

because they knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiff and Class Members.

151. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

152. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiff and Class Members to suffer damages.

153. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

154. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Classes)

155. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

156. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class Members agreed to provide their Private Information to Defendant, and Defendant agreed to provide medical services for monetary compensation and, impliedly if not explicitly, agreed to protect Plaintiff's and other Class Members' Private Information.

157. These contracts include, but are not limited to, test requisition forms, patient signature cards, HIPAA authorization forms, and patient consent forms.

158. To the extent Defendant's obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

159. A meeting of the minds occurred, as Plaintiff and other Class Members agreed, among other things, to provide their Private Information, and allow Defendant to provide medical services for monetary benefit, in exchanges for Defendant's agreement to protect the confidentiality of that Private Information.

160. The protection of Plaintiff's and other Class Members' Private Information were material aspects of Plaintiff's and other Class Members' contracts with Defendant.

161. Defendant's promises and representations described above relating to HIPAA, and industry practices, and about Defendant's purported concern about their patients' privacy rights became terms of the contracts between Defendant and their patients, including Plaintiff and other Class Members. Defendant breached these promises by failing to comply with HIPAA, and reasonable industry practices.

162. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Shields and/or otherwise understood that Shields would protect its patients' Private

Information if that information were provided to Shields.

163. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

164. As a result of Defendant's breach of these terms, Plaintiff and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and other Class Members have been put at risk of future harm, which may take months if not years to manifest, discover, and detect.

165. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes, in the Alternative to Count III)

166. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

167. Plaintiff and Class Members were required to provide their Private Information, including their names, Social Security numbers, addresses, medical record numbers, dates of birth, telephone numbers, email addresses, and various health related information to Defendant as a

condition of their use of Defendant's services. By providing their Private Information, and upon Defendant's acceptance of such information, Plaintiff and all Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, services to be provided by Defendant to Plaintiff.

168. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiff's and other Class Members' Private Information. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their Notice of Privacy Practices and other public statement described above.

169. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their health information and other Private Information from unauthorized disclosure.

170. In their written privacy policies, Shields expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

171. Shields promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

172. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information was Defendant's obligation to (a) use such Private Information for business purposes only; (b) take reasonable steps to safeguard that Private Information; (c) prevent unauthorized disclosures of the Private Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiff and Class

Members from unauthorized disclosure or uses; and (f) retain the Private Information only under conditions that kept such information secure and confidential.

173. Without such implied contracts, Plaintiff and Class Members would not have provided their Private Information to Defendant.

174. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

175. Defendant breached the implied contracts with Plaintiff and Class Members by failing to conduct the following:

i. reasonably safeguard and protect Plaintiff's and Class Members' Private Information, which was compromised as a result of the Data Breach;

ii. comply with their promise to abide by HIPAA;

iii. ensure the confidentiality and integrity of electronic protected health information that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R 164.306(a)(1);

iv. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);

v. implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R 164.308(a)(1);

vi. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii); and

vii. protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2).

176. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and other Class Members have suffered a variety of damages including but not limited to:

the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, to monitor medical records, and health insurance information, and to file police reports; and Plaintiff and other Class Members have been put at risk of future harm, which may take months if not years to manifest, discover, and detect.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

177. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

178. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

179. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

180. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management

and security.

181. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

182. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

183. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

184. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

185. Plaintiff and Class Members have no adequate remedy at law.

186. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued

possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

187. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

188. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Classes)

189. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

190. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class Members' PII and/ PHI. Defendant has become a fiduciary, created by its undertaking and guardianship of patients' Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

191. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to conduct the following:

i. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' Private Information;

ii. timely notify and/or warn Plaintiff and Class Members of the Data Breach;

iii. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R 164.306(a)(1);

iv. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);

v. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R 164.308(a)(1);

vi. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii);

vii. protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2);

viii. protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R 164.306(a)(3);

ix. ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R 164.306(a)(94);

x. prevent the improper use and disclosure of protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R 164.502, *et seq.*;

xi. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R 164.530(b) and 45 C.F.R 164.308(a)(5);

xii. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R 164.530(c); and otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

192. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect patients' Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

193. As a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VII
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

194. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

195. At all times during Plaintiff's and Class Members' interactions with Defendant,

Defendant was fully aware of the confidential nature of the Private Information that Plaintiff and Class Members provided to Defendant.

196. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to the unauthorized third parties.

197. Plaintiff and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

198. Plaintiff and Class Members also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of protecting their networks and data systems.

199. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

200. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was knowingly and/or voluntarily disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

201. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

202. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

203. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' Private Information had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' Private Information in jeopardy.

204. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Defendant's services they received.

205. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VIII
MAINE UNFAIR TRADE PRACTICES ACT,
5 Me. Rev. Stat. §§ 205, 213, *et seq.*
(On Behalf of Plaintiff and the Maine Sub-Class)

206. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

207. Shields is a "person" as defined by 5 Me. Stat. § 206(2).

208. Shields' conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

209. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

210. Shields engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

ii. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

iii. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

vi. Failing to timely and adequately notify Plaintiff, and Maine Subclass members of the Data Breach;

vii. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

viii. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

211. Shields' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Shields' data security and ability to protect the confidentiality of consumers' Private Information.

212. Shields' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Maine Subclass members, that their Private Information was not exposed and misled Plaintiff and the Maine Subclass members into believing they did not need to take actions to secure their identities.

213. Had Shields disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Shields would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Shields was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Maine Subclass. Shields accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Shields held itself out as maintaining a

secure platform for Private Information data, Plaintiff, the Class, and the Maine Subclass members acted reasonably in relying on Shields' misrepresentations and omissions, the truth of which they could not have discovered.

214. As a direct and proximate result of Shields' unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

215. Plaintiff and the Maine Subclass members seek non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

216. Plaintiff intends to send a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) and intends to amend this complaint to seek monetary damages pursuant to the pre-suit notice requirement.

COUNT IX
MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT, 10 Me. Rev. Stat. §§ 1212, *et seq.*
(On Behalf of Plaintiff and the Maine Sub-Class)

217. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

218. Shields is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

219. Shields advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

220. Shields engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

i. Representing that goods or services have characteristics that they do not have;

ii. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

iii. Advertising goods or services with intent not to sell them as advertised; and

iv. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

221. Shields' deceptive trade practices include:

i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

ii. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

iii. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

vi. Failing to timely and adequately notify Plaintiff, and Maine Subclass members of the Data Breach;

vii. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

viii. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

222. Shields' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Shields' data security and ability to protect the confidentiality of consumers' Private Information.

223. Shields' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Maine Subclass members, that their Private Information was not exposed and misled Plaintiff and the Maine Subclass members into believing they did not need to take actions to secure their identities.

224. Shields intended to mislead Plaintiff and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

225. Had Shields disclosed to Plaintiff and Maine Subclass members that its data systems were not secure and, thus, vulnerable to attack, Shields would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Shields was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, and the Maine Subclass. Shields accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Shields held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Maine Subclass members acted reasonably in relying on Shields' misrepresentations and omissions, the truth of which they could not have discovered.

226. As a direct and proximate result of Shields' deceptive trade practices, Plaintiff and

Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

227. Maine Subclass members are likely to be damaged by Shields' ongoing deceptive trade practices.

228. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT X
MAINE CONFIDENTIALITY OF HEALTH CARE INFORMATION LAW, 22 M.R.S. § 1711-C
(On Behalf of Plaintiff and the Maine Sub-Class)

229. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

230. The Maine Confidentiality of Health Care Information law prohibits, among other things, unauthorized disclosure of patient health care records. 22 M.R.S. § 1711-C (2).

231. Plaintiff provided her PHI to Shields which is a "health care practitioner" as defined by 22 M.R.S. § 1711-C (1)(F).

232. Shields is a "health care practitioner" as defined by 22 M.R.S. § 1711-C (1)(F).

233. Plaintiff is an "individual" whose health care information was disclosed without proper authorization as defined by 22 M.R.S. § 1711-C (1)(G).

234. Shields had a duty to develop and implement policies, standards and procedures to protect the confidentiality, security and integrity of the Plaintiff's and the Maine Subclass

member's health care information to ensure that information is not negligently, inappropriately or unlawfully disclosed. 22 M.R.S. § 1711-C (7).

235. Shields disclosed health care information pertaining to the Plaintiff and the Maine Subclass without their consent and for no other reason permitted by 22 M.R.S. § 1711-C.

236. Unauthorized disclosure of health care information to hackers resulted from the affirmative actions of Shields in maintaining the security of its computer system at levels that did not protect the confidentiality, security and integrity of the Plaintiff's and the Maine Subclass member's health care information and allowed hackers to improperly access and copy private health care information of the Plaintiff and the Maine Subclass.

237. The affirmative actions of Shields in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private health care information of the Plaintiff and the Maine Subclass. Shields actively and affirmatively allowed the hackers to see and obtain the health care information of the Plaintiff and members of the Maine Subclass.

238. Plaintiff and the Maine Subclass members were injured and have suffered damages from Shields' illegal disclosure and release of their health care information in violation of 22 M.R.S. § 1711-C (2).

239. Plaintiff individual and on behalf of the Maine Subclass seeks relief including but not limited to actual damages, injunctive relief, and/or attorneys' fees and costs under 22 M.R.S. § 1711-C (13)(B).

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the sub-class, as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff

is a proper class and sub-class representative; and appoint Plaintiff's Counsel as Class and Sub-class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Shields from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and members of the Class and Sub-class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Shields as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: July 27, 2022

Respectfully submitted,

BERMAN TABACCO

/s/ Patrick T. Egan

Patrick T. Egan (BBO 637477)
Nathaniel L. Orenstein (BBO 664513)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
norenstein@bermantabacco.com

Melissa R. Emert (*pro hac vice* forthcoming)
Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Tel: (201) 391-7000
Fax: (201) 307-1086
memert@kgglaw.com
ggraifman@kgglaw.com

Lynda Grant
THEGRANTLAWFIRM, PLLC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Tel: (212) 292-4441
Fax: (212) 292-4442
lgrant@grantfirm.com

Attorneys for Plaintiff and the Class

Of counsel:

Jeffrey Neil Young
Solidarity Law
9 Longmeadow Road
Cumberland, ME 04110
Tel: (207) 844-4243
jyoung@solidarity.law